ISSUE 51 APRIL 2022

RJ2 TECHNOLOGIES

Newsletter

What's Inside:

Password Tips To Keep Your Data Safe
Page 01-03

Why Managed IT Services Is Best For SMB Cybersecurity:
Page 04

Use These Web Browsers To Secure Your Date
Page 05

Your SMB Will Enjoy the Flexibility Provided By Hybrid Cloud Platforms:
Page 06

This monthly publication provided courtesy of Jeff Dann, President of RJ2 Technologies.

Password Tips To Keep Your Data Safe

No matter what application, account, or platform that you have a login for, you want to make sure your passwords are not leaving you vulnerable. Whether it's for personal or professional purposes, you need to protect your sensitive data and how it can be accessed. Cybercriminals will continue to think of new and innovative ways to hack accounts. How can you get ahead of cybercriminals, data breaches, and botnets? Weak passwords can have serious consequences, especially if your business handles sensitive information of your clients and/or employees. You need to create strong, unique passwords. What exactly does that mean though? There are some simple and easy password tips for data security that you can follow.

DO'S

What does a unique and strong password actually entail? You will want to think beyond just creative, cute, or funny phrases. You also should incorporate upper- and lower-case letters, symbols, punctuation, and/or numbers. Here is one way you can go about landing on a strong and unique password: settling on a creative phrase and replacing some of the letters with numbers, interchanging letters between upper and lowercase letters, and inserting characters along the way.

For example, let's say your creative phrase is "Nobody Is Welcome." As a potential password it could look like "N06od3<1z>W3lc0m$." It may not be easy to memorize; however, it is a better option for your security and safety of information. Secure passwords commonly include random characters, numbers, and letters to make a more complex password. These are just a few password tips for data safety that you can use in the office and/or at home.

Continued on Page 2

CONTINUED...

You will want to prioritize your password length as well. Try having at least 16 characters in your password. This will help lessen the chances of falling victim to a cyberattack or data breach of any sort.

Businesses and individuals utilize Password Managers (a kind of virtual vault) that individuals use to store and automatically insert your password when accessing certain account. These products can help you organize your passwords for different applications to avoid using the same password on multiple accounts. They have integrations with most common cloud sites and applications. Some of these can be sophisticated creating very complex passwords, and then change that password after ever use automatically. This is important so if your hacked, any passwords left in cache or elsewhere in your computer is inactive and unusable by the hacker. These are very secure methods using technology to move away from phrases, but the price tag can be challenging for individuals.

Another great tip is to always use two-factor authentication (2FA). Requiring you to enter a multi digit code that is texted to your smartphone to enter as a requirement to login to any account. These solutions include applications like Authy, Google Authenticator, and Microsoft Authenticator at the basic level however there are more enterprise level solutions available. Two factor authentication makes it significantly harder to gain access into your account, even if they have your password.

Also, get a service to monitor your email account on the dark web. If your email address and password have been compromised, hackers will post your credentials on the Dark Web and sell them to anyone interested. The monitoring the Dark Web will tell you if your email address has been posted and notify you to change your passwords immediately. More on this below.

DON'TS

Now that we know a few password tips for data safety, what are some things to avoid? First things first, never use personal information. Phone numbers, addresses, names, and birthdays should be avoided. Also, as a general rule, don't save your password in the application you're using so you don't have to remember and enter it each time you go to the site. Many sites will offer that as an option when you login. This is a bad practice, and you should investigate using a Password Manager if this is an issue for you.

Second, you will want to steer clear of repeating passwords. This does not make it easy for your memory however, reusing the same password for multiple accounts puts you at a greater risk for credential stuffing attacks. Credential stuffing attacks are when cybercriminals search the dark web for stolen login credentials, then they attain a massive list of stolen usernames and passwords. Following that, a botnet tests the stolen credentials against multiple sites at once, and the working credentials are then used to steal private information from all vulnerable users. Recycling is generally a good act to practice except when it comes to your passwords. Plus, if you know that a password has been compromised at any point, you should avoid using that password ever again. All the more reason to lower your susceptibility with a stronger, longer, and unique password for your login.

Another one of our password tips for data safety is to avoid using real words, even if it's an uncommon word in the thesaurus. Why? There are malicious programs that hackers use to process every word found in a dictionary to crack passwords. One key element to stay away from is using proper nouns and other standalone dictionary words. You will also want to be careful what you share and who you share it with when it comes to your passwords.

If you have not checked or changed your privacy settings on your social media accounts, now may be the time. Most people enjoy posting personal details about themselves, their family, their whereabouts, and lifestyle. There's nothing inherently wrong with doing so; however, you should change your privacy setting to restrict all your posts to only your real-life "friends." This not only protects you, but also your family's personal information, kids' personal information, and so much more. Allowing strangers to follow your personal accounts leaves you vulnerable to malicious content such as clicking phishy links from a source you thought was your friend. This could give that hacker your password credentials and if you use the same password across multiple accounts, you risk having all your social media platforms being hacked.

Continued on Page 3.

CONTINUED...

OTHER PASSWORD TIPS FOR DATA SAFETY

There are several other password tips for data safety that you can add to your list. You can opt for a secure password manager, which will vault your login information for you. A good portion of password managers available have extra security measures in place. You should consult with your managed services provider to find the right match for your needs in your business. A few other tips would be to randomize patterns and sequences in creating your password, avoid public Wi-Fi as much as possible when using company property, check your password strength, and change passwords periodically. No matter what you do, you will never be fool proof from a data breach or cybercriminal. It is wise to have a backup and disaster recovery plan in place. In the scenario where your company suffers from data loss, you need a plan and a capable team in place and ready to move. It is truly an essential piece for your business to have a backup and disaster recovery plan. Your managed services provider can create an exceptional and tailored plan that will cover your specific needs.

CONCLUSION

If you want more information regarding more password tips for data safety, password managers, or backup and disaster recovery plans that will benefit you and your organization, contact us today. Consult with a managed services provider that cares about their clients, works as an extension of your team, and provides quality services. Regardless of your business size, the benefits of a long-term relationship with a knowledgeable and reliable provider are essential for creating a thriving company. RJ2 Technologies can provide that to you.

RJ2 SPOTLIGHT

Shawn Meyer:

Director of Corporate IT

Shawn has over 20 years of experience in utilizing various technologies for implementation, management, and administration of Fortune 100 Enterprise level distributed environments. As part of the management team, Shawn oversees Enterprise IT and Consulting engagements for RJ2 Technologies' clients.

Prior to RJ2 Technologies, Shawn was the regional IT manager for a large entertainment corporation and was recognized for his change management Leadership during a complex system wide conversion to digital media. In addition, Shawn has worked with various clients throughout the Chicago land area.

Shawn enjoys spending time with his wife and three energetic kids and volunteers for a variety of nonprofit organizations in the Chicago land area.

FEATURED PARTNER

SKYCOM

Easily accessible via any modern web browser or mobile device, our feature rich phone system helps to improve your communications, streamline your business processes, and facilitates your growth and success.

As your needs grow and change over time, so do our features and capabilities. Endlessly scalable, flexible, and reliable, our cloud communications platform is truly future-proof, so you can focus on your business, and know that your communications solution will always remain relevant and competitive.

Why Managed IT Services Is Best For SMB Cybersecurity

Businesses thrive on technological advancements and are constantly looking to upgrade their outdated tech. However, as technology continues to improve, so do the skills of threat hackers and cybercriminals. This is why it is very important that small- and mid-sized businesses (SMB) take the proper steps to protect themselves from cyber crime through managed IT services. A great way to do this is to outsource your IT needs to a group of trusted professionals called a managed service provider (MSP). MSPs like RJ2 Technologies ensure that your SMB is receiving proper IT support while monitoring and protecting your company from cybercriminals.

THE NUMBERS:

Over the last decade, the number of cyberattacks on SMBs has risen drastically and we have seen an even larger increase in these attacks in the pandemic years. Many SMBs face attacks such as misconfigured systems, ransomware attacks, credential stuffing, and even social engineering. According to Verizon's 2021 Data Breach Investigations Report just about one in every five victims of a data breach attack was a SMB. Another scary statistic is that only 47% of SMBs are able to detect a cyber attack or data breaches within a few days timespan. This gives hackers and cybercriminals lead way and a lot of time to steal you data with malicious intent.

Not only have the frequency of cyber attacks risen, but so have the financial consequences associated with these attacks. According to IBM's Cost of a Data Breach Report 2021, "data breach costs rose from USD 3.86 million to USD 4.24 million."

As you can see, the numbers don't lie. It is crucial for SMBs to start taking cybersecurity seriously as they are more likely to be hacked, do not have adequate cybersecurity measures in place, and cannot afford for their business to be down for days-weeks at a time. Not to mention the financial consequences that come with the time consuming task of cleaning up the mess left over.

Your SMB can take proactive measures by reaching out to a MSP near you to discuss the security of you company and what can be done moving forward.

WHY MANAGED IT SERVICES:

The best way to prevent cyber harm to you business is by partnering with a trusted MSP to protect and defend your business from malicious attacks.

Managed service providers specialize in many different areas of expertise such as IT Network Solutions, Data Protection, Unified Communications, Cyber Security, Backup and Disaster Recovery and many other services to provide you with around the clock support. Here is a more detailed list of what MSPs can offer your SMB:

- **24/7 Monitoring:** Cyber criminals don't work the regular 9-5, they work around the clock. This is why MSPs like RJ2 Technologies offer 24/7/365 support to ensure that your company is protected at all hours of the day.
- **Data Encryption**: Data encryption is the process of making data unreadable through the use of hashing or other encryption methods. Encryption uses keys (Private or Public or both) to ensure that your data is only being read by the end users and not anyone else in-between.
- **Backup and Disaster Recovery:** MSPs make constant and consistent backups of your valuable data to make sure you never lose what is important to you. By making regular backups, MSPs can save your valuable data in the cloud to be retrieved in the event of a cyber attack or a simple human error.
- **Real-Time Threat Prevention and Elimination:** MSPs utilize technology that enables them to detect and stop threats as they happen. This minimizes the impact of an attack and keeps your data safe.
- **Network and Firewall Protection:** Networks and firewalls create a barrier between your business network and the internet. They secure confidential data from the outside, protecting you personal info like credit card numbers, addresses, employee records, or other valuable data you wouldn't want the world to know.
- **Security Awareness Training:** MSPs offer security awareness training for your company's employees to ensure you are practicing good cyber habits. Did you know that the majority of cyber attacks are a direct result of human error? Part of our training involves teaching your employees the basics and running simulations to test their knowledge.

Managed Service Providers (MSPs) main goal is to help small and medium sized businesses get all their IT needs in order. This involves utilizing a help desk to be there for your employees IT questions and needs. It also involves protecting your company from outside harm, making sure your data is backed up, putting disaster plans in place, and unifying your communications throughout your business.

If your company isn't protected from cyber attacks and you cannot afford to be out of business for extended periods of time, contact a managed service provider near you such as RJ2 Technologies. MSPs will ensure your company is safe and all your IT needs are met so you can focus on your business. Don't wait for an attack to happen to you, be proactive!

Use These Web Browsers To Secure Your Data

Web browsers are types of application software that connect you to the internet. When you request information, the browser is responsible for retrieving the necessary content from the world wide web, and displaying it on your device in front of you. As cybercrimes become more widespread, you will need a competent web browser packed with security features that will protect you from malicious harm while searching the internet. We have put together a list of a few good browsers that are safe and come with great security features.

TOR BROWSER

Tor is the top choice for web browsers when it comes to protecting your privacy. This browser was developed by the famous Edward Snowden, former computer intelligence consultant. Some of the benefits associated with Tor are:

No one will be able to watch your internet activity such as the web pages you visit.
It protects your IP address from website operators by showing a connection from "Tor" instead of your real IP address. Basically, no one will no it is you unless you put your credentials out there.
To keep you completely anonymous, Tor implements many different layers of encryption on your traffic

BRAVE

Brave was developed by JavaScript creator Brendan Eich, and this web browsers main feature is ad blocking. Brave automatically blocks ad trackers and will even go as far as replacing that web pages ads with ads of its own. This is a nice feature since you will not see targeted cookie ads while searching the internet but instead will see ads from Brave. Another great feature is it will not auto-collect your data which allows Brave users to keep their personal data private from potential cybercriminals.

MOZILLA FIREFOX

Unlike Google Chrome or Safari, Firefox is open source, which means cybersecurity experts can review its source code for any potential vulnerabilities. Firefox recently added a new feature called HTTPS-Only Mode. This mode helps to keep your internet activates more secure by only connecting you to websites that are secure. Here are some of the other protection benefits:

- Blocks anyone looking to track you online
- Anti-fingerprinting
- Breached website alerts
- Improved tracking protection

EPIC

Epic browser was developed with built-in safeguards against third-party widgets, cryptocurrency mining scripts, cookies, and ad tracking scripts. It connects to the internet using an encrypted proxy server to hide a user's browsing activity and IP address.

Epic is also designed to block calls that carry the risk of leaking your IP address, even if you're using a virtual private network (VPN). Lastly, this browser comes with a feature that allows users to see who's tracking them and what trackers have been blocked.

The key to protecting your online data and browsing the internet safely is a secure browser. As to what constitutes as the "best" secure browser depends largely on the needs of your organization. Visit RJ2 Technologies to learn more about protecting your data and how they can help you mitigate risk when surfing the internet.

TIPS OF THE MONTH

1. If you're at an airport and need to connect to Wi-Fi, you can log in by simply adding "?.jpg" to the end of the URL.

2. If you want to save part of your screen as an image without taking a screenshot of the entire page, hold "Ctrl" + "Shift" + "S" to drag a customizable snippet.

3. Quickly clear your cache by holding "Ctrl" + "Shift" + "R".

4. In Excel, create better tables by selecting" format as table" then choose which option you like best. This will allow your table to have customizable drop down menus with headers as well.

Your SMB Will Enjoy The Flexibility Provided By Hybrid Cloud Platforms

Hybrid cloud platforms are a great way to improve a business's agility and flexibility, as they can be used to host business components in an affordable and low-impact manner. But what exactly is the hybrid cloud, and what are its specific advantages for small- and medium-sized businesses (SMBs)? Read on to learn more.

Hybrid clouds are a combination of private and public clouds. In private clouds, data and applications that require tighter controls are hosted either internally or privately on an off-site facility. Meanwhile, public clouds are managed externally by third-party providers with the express purpose of streamlining a company's IT infrastructure.

BENEFITS OF A HYBRID CLOUD SETUP

Here are three significant advantages of hybrid cloud environments.

Adaptability:
Having the ability to choose between internally or privately hosted cloud servers and public ones lets you pair the right IT solution with the right job. For example, you can use the private cloud to store sensitive files while utilizing more robust computing resources from the public cloud to run resource-intensive applications.

Cost efficiency and scalability:
Does your business struggle to meet seasonal demands? With a hybrid cloud solution, you'll be able to easily handle spikes in demand by migrating workloads from insufficient on-premises servers to scalable, pay-as-you-go cloud servers whenever needed, without incurring extra hardware and maintenance costs.

So if there are last-minute computing demands that your hardware can't support, or if you're planning for future expansion, you can easily scale capacity up or down with a hybrid cloud solution.

Security:
Last but not least are the security advantages of a hybrid cloud solution. You can host sensitive data such as eCommerce data or an HR platform within the private cloud, where it will be protected by your security systems and kept under close watch. Meanwhile, routine forms and documents can be stored in the public cloud and protected by a trusted third party.

HOW TO SET UP A HYBRID CLOUD

The following are the different ways to set up a hybrid cloud model based on your SMB's requirements and the providers available to you:

- Employ one specialized cloud provider who offers comprehensive hybrid solutions.
- Integrate the services of a private cloud provider with those of another public cloud provider.
- Host a private cloud yourself and then incorporate a public cloud service into your infrastructure.

Our experts can help you transition to a hybrid cloud solution without interruption and huge costs. Contact us today to learn more about the business benefits of a hybrid cloud.

CONTACT US TODAY!

Our Role:

- We manage your IT services to help improve your business' ROI
- RJ2 Technologies creates a customizable plan for your business' needs no matter the size or budget
- We assist with designing and implementing new technologies, focused on expanding your business

For more information on how RJ2 Technologies can help your business grow contact us now at: https://rj2t.com/contact/ or give us a call at (847) 303-1194